METHODS AND SYSTEMS FOR PROVIDING CONVERGED NETWORK MANAGEMENT FUNCTIONALITY IN A GATEWAY ROUTING NODE

AN APPLICATION FOR

UNITED STATES LETTERS PATENT

By

Dan Alan Brendes
Raleigh, North Carolina

Joseph William Keller
Cary, North Carolina

Seetharaman Khadri
Durham, North Carolina

"Express Mail" mailing number EK929856672US
Date of Deposit January 26, 2001
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C F R 1 10 on the date indicated above and is addressed to the Commissioner of Patents, Washington, D C 20231
Karen S. Flynn

Description

METHODS AND SYSTEMS FOR PROVIDING CONVERGED NETWORK MANAGEMENT FUNCTIONALITY IN A GATEWAY ROUTING NODE

Priority Application Information

This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/208,523 entitled *Methods and Systems for Distributing SS7 Network Management Messages to IP Nodes*, filed June 1, 2000, the disclosure of which is incorporated herein by reference in its entirety.

Technical Field

The present invention relates to the distribution of network management information in a non-homogeneous communications network environment, and more particularly to methods and systems for generating and routing network management type signaling messages in a network environment that employs both a signaling system 7 (SS7) message transfer part (MTP) based network component and an Internet protocol (IP) based network component.

Background Art

In modern telephony networks, service control points (SCPs) serve as an interface to telephony related databases, such as: call management service

databases (CMSDB); line information databases (LIDB); and business services databases (BSDB). These databases are used, at least in part, to facilitate a variety of intelligent network (IN) type services including: find me service, follow me service, computer security service, call pickup service, store locator service, call waiting service, call block service, calling name delivery service, three way calling service, 800 number services, etc. Such telephony service databases may also be employed to provide communication service subscribers the flexibility to easily port their service from one communication service provider to another (i.e., number portability or local number portability).

It will be appreciated that the application of such SCP-type database services is not limited to the traditional wired public switched telephone network (PSTN), but is also widely implemented in the wireless telecommunications industry. Typical wireless network communication database applications include: home location registers (HLRs), visitor location registers (VLRs), authentication centers (AuCs), short message service centers (SMSCs), and equipment identification registers (EIRs). The term SCP is commonly used to broadly refer to a network element that includes a database system for providing database-intensive services, such as those discussed above.

It will also be appreciated that with the continuing convergence of traditional telecommunication networks and traditional data networks, the number and variety of converged or inter-network service related database applications designed to service the needs of combined data-telecommunications subscribers (e.g., presence service databases, telephony-

to-WWW domain name servers, etc.) will increase dramatically in the future. As this converged network environment continues to evolve, so will the tendency of network operators to place SCP-like database nodes within the data network component of the converged network environment. That is to say, PSTN and wireless telephone network operators will likely find the economics of data network operation favorable to the placement of SCP-like database nodes within the data sub-network of the converged network environment, as opposed to the traditional PSTN – signaling system 7 (SS7) sub-network. As such, SCP and SCP-like network elements that have traditionally resided within an SS7 signaling network and been assigned a unique SS7 network address (point code and subsystem) would instead be placed within a data network, such as a transmission control protocol / Internet protocol (TCP/IP) based network, and would consequently be assigned an Internet protocol (IP) network address, hostname, and port number.

It will also be appreciated that in addition to database nodes, the convergence of telephony and data networks has led to the advent of numerous network elements that are associated with call setup and teardown functions which reside in or on the edge of the data network component of the converged communications network environment. Such network elements include media gateways (MGs), media gateway controllers (MGCs), and softswitch (SS) nodes, all of which are well known to those skilled in the art of Internet telephony. These nodes typically communicate using a data network based

protocol (e.g., TCP/IP) in a manner similar to that of the SCP and SCP-like database nodes discussed above.

Shown in Figure 1 is a sample converged communication network, generally indicated by the numeral **100**. Converged network **100** includes a signaling system 7 (SS7) network component and an Internet protocol (IP) network component. The SS7 network component includes a service control point (SCP) **104**, a signal transfer point (STP) **106**, and an end office (EO) or service switching point (SSP) **108**. It will be appreciated that these SS7 nodes are connected via dedicated SS7 communication links, and consequently communicate using SS7 formatted signaling messages. The IP network component includes an IP based database server (DBS) **112**, a first media gateway controller (MGC) **114**, and a second MGC **116**. These IP nodes are connected via IP communication links, and consequently communicate using IP formatted signaling messages. A signaling gateway node (SG) **120** facilitates inter-network communication. SG **120** is adapted to communicate via one or more SS7 links with the SS7 network component, while simultaneously communicating with the IP network component via one or more TCP/IP connections or sockets. SG **120** provides a degree of signaling message protocol translation, such that signaling messages originating in the IP network may be properly communicated to the appropriate destination node in the SS7 network, and vice versa.

An example of this inter-network message communication functionality is also provided in Figure 1. In this example, MGC node **116** formulates and

transmits an IP-based query message, **Q**, that is ultimately destined for SCP node **104** in the SS7 network. However, it will be appreciated that the SS7 and IP sub-networks are separate and distinct entities that have a limited knowledge of each other's architecture or communication protocols. The query message passes through the IP network and eventually arrives at the signaling gateway node **120**, where it is received, processed, and re-formatted into a form suitable for transmission through the SS7 network. A new SS7 query message, **Q***, is subsequently generated and routed via STP **106** to the destination node, SCP **104**. In response, SCP **104** generates an SS7 reply message, **R***, which is routed via STP **106** back to SG **120**. SG **120** again receives, processes, and re-formats the reply message into a form that is suitable for transmission through the IP network. The new IP reply message, **R**, is subsequently routed through the IP network back to MGC **116** in response to the original query.

The converged network architecture described above functions reasonably well; however, efficient and effective network management can become a significant problem in such networks. This difficulty arises from the same basic issue that was raised previously with regard to message routing; i.e., the SS7 and IP sub-networks are separate and distinct entities which have a limited knowledge of each other's architecture, communication protocols, and network management procedures.

With particular regard to the issue of network management, in a traditional SS7 signaling network there exist three categories of network management: traffic management, link management, and route management.

Traffic management is the process of diverting messages away from failed links, while link management involves the activation and deactivation of signaling links. Route management is responsible for both re-routing messages around failed SS7 signaling points and controlling the flow of messages to any given signaling point in the network. Those skilled in the art of SS7 signaling network operation will appreciate such a network management strategy provides a layered approach to managing anomalistic events in an SS7 network. The SS7 protocol provides procedures designed to minimize the effects of network congestion and outages from the link level all the way up to the route level. Within the SS7 message transfer part (MTP) protocol, level two facilitates the detection of errors on individual signaling links. Level two is not concerned with communication abnormalities that arise outside the signaling point, but instead is adapted to resolve those issues associated with an individual signaling link. Again, it will be appreciated that every SS7 signaling link incorporates this function, which is controlled by level-three link management.

When an error is encountered, level two reports the error to level three, which in turn must then determine which error resolution procedures to invoke. In general, SS7 error resolution procedures begin at the lowest level, the link level, and work their way up to the highest level, the route level. While these procedures do not have a direct impact on routing or the status of signaling points, they do, however, trigger other level-three network management events.

Traffic management is effected by link management, primarily because traffic management must divert traffic away from a link that link management has failed and removed from service. For example, each SS7 signaling link may have a link buffer that stores messages to be transmitted. Once an acknowledgement is received from the receiving node, the corresponding message can be over-written or removed from the link buffer. If a message is not acknowledged within a predetermined time period, it will be retransmitted. Thus, messages must be stored in the link buffer until they are acknowledged.

When a signaling link fails, its associated link buffer in the transmitting node may contain many unacknowledged messages because the original messages may not have reached the destination or the acknowledgements may not have reached the source. Traffic management diverts traffic from the failed link to a new link and copies any unacknowledged messages from the link buffer associated with the failed link to the link buffer for the new link. The unacknowledged messages transferred to the new link buffer may then be retransmitted. In this manner, traffic management ensures the orderly delivery of all diverted traffic.

It should be noted that the traffic management process does not divert traffic away from a signaling point. The purpose of traffic management is simply to redirect traffic at a signaling point to a different signaling link associated with the signaling point. It is true, however, that the traffic management process does impact routes and route-sets to specific destinations. If a particular route is used by another signaling point to reach a destination, and traffic

management has diverted traffic away from that route, adjacent signaling points may have to invoke route management procedures.

At the highest level, route management, unlike traffic management, diverts traffic away from signaling points that have become unavailable or congested. Regardless of the root cause, traffic management and link management will be involved at the affected signaling point. At the same time, all the signaling points around the affected signaling point are forced to invoke route management procedures to prevent messages from becoming lost.

In an SS7 network the above-described network management functionality is accomplished, in part, through the use of specific network management messages. A sample structure of a typical SS7 network management message or message signaling unit (MSU) **150** is illustrated in Figure 2. It will be appreciated by those skilled in the art of SS7 signaling communications that signaling information field (SIF) **152** of MSU **150** contains data associated with a particular point code that is experiencing difficulty or a particular link that has failed. Additional status information, priority codes, and other relevant maintenance codes may also be included in SIF parameter **152**, depending upon the particular type of network management message being sent.

There are a number of routing management messages that are commonly employed to re-direct traffic around a failed or congested route. Again, it will be appreciated that such messages may be sent by an SS7 signaling point in response to the failure of one or more provisioned links. More

particularly, when a route fails, a routing management message is sent to all neighboring SS7 signaling nodes (i.e., those SS7 signaling nodes that are adjacent to the troubled signaling node). This routing management message informs the neighboring SS7 signaling nodes of the problem at the troubled node and also provides instructions regarding future routing to the troubled node. It will also be appreciated that routing management messages are also used to inform neighboring SS7 signaling nodes of the recovery of a previously troubled node. Such SS7 routing management messages include: transfer prohibited (TFP), transfer restricted (TFR), transfer controlled (TFC), transfer allowed (TFA) messages, transfer cluster prohibited (TCP), and transfer cluster allowed (TCA). These messages are only a subset of all network management messages defined in the SS7 protocol. A comprehensive discussion of SS7 network management and related issues can be found in *Signaling System #7* by Travis Russell, McGraw-Hill Publishing 1998.

A transfer prohibited (TFP) message is generated and transmitted by an SS7 signaling point (e.g., an STP) in response to determining that communication with an SS7 node is no longer possible. In response to determining that communication with an SS7 node is possible, but sub-optimal, a transfer restricted (TFR) message is sent. A TFR message essentially requests that adjacent SS7 signaling points use alternate routes when sending messages to the troubled SS7 node. If alternate routes are not available, messages may continue to be routed normally. A transfer controlled (TFC) message is sent by an SS7 signaling point (e.g., STP) in response to the

receipt of an MSU that is destined for a congested route. In such a scenario, the MSU is discarded and a TFC message is returned to the originator or sender of the MSU. A transfer allowed (TFA) message is sent by an SS7 signaling point when a previously failed route once again becomes available.

Shown in Figure 3 is a scenario involving network management message flow in converged communications network **100** described above with regard to Figure 1. In this example, it is assumed that the SS7 communication link that connects STP **106** and SCP **104** has failed. In response to the detection of this failure, STP **106** transmits a transfer prohibited (TFP) network management message to each of it's neighboring SS7 signaling points, SSP **108** and SG **120**. Consequently, both SSP **108** and SG **120** are made aware that they should not attempt to send any SS7 MSU traffic to SCP **104** via a route that involves STP **106**.

It will be appreciated that, in the absence of such proactive network management procedures, SSP **108** and SG **120** might flood STP **106** with MSUs as a result of continuous, repeated attempts to obtain a response from the failed or inaccessible SCP **104**. In such a scenario, STP **106** could incur significant congestion that might interfere with or prevent the routing of messages to other available SS7 signaling nodes in the network. As such, it is possible that the failure of one node in the network could potentially lead to the failure of another, and so on. It is precisely this situation that SS7 network management procedures are designed to prevent.

Given the discussion above, a significant problem encountered with converged networks now becomes more apparent. As shown in Figure 3, SSP **108** and SG **120** are notified that they should no longer send messages to SCP **104**. However, since nodes in the IP component of the converged network are not capable of directly receiving and interpreting SS7 messages, there is no method of notifying any IP nodes in the IP sub-network that messages destined for SCP **104** should not be sent. Those skilled in the art of IP network operation will appreciate that some transport and higher layer protocols in the IP protocol stack employ periodic retransmission of messages if no response or acknowledgment is received within a pre-defined acknowledgment interval. As such, SG **120** may become flooded with re-transmitted query messages, destined for SCP **104**, from nodes within the IP network. Again, it will be appreciated by those skilled in the art of communication network operations that such a scenario can have significant adverse impacts on the overall viability of the converged network.

Therefore, what is needed is a system and method of extending network management functionality in converged communication network environment such that anomalistic events, and any subsequent resolution procedures, occurring in one sub-network component of the converged network can be effectively communicated to another sub-network component of the converged network.

Disclosure of the Invention

The present invention includes a communications network element that is capable of routing messages and also performing inter-network management functions in a converged telephony-data network environment. In one embodiment, the present invention is implemented in the form of a signaling gateway routing node which is adapted to facilitate signaling communication between nodes in a signaling system 7 network and nodes in an Internet protocol (IP) network. In addition to basic message routing functionality, the signaling gateway routing node is adapted to notify nodes in the IP network when a node in the SS7 network becomes congested or unavailable. In certain cases, the signaling gateway selectively notifies only IP nodes that are concerned with the status of the troubled SS7 node; while in other cases, notification messages are broadcast to all relevant IP nodes. The signaling gateway also serves to limit the number of status queries or polling messages that are conveyed from IP nodes through to the distressed SS7 node, thereby reducing needless congestion in the SS7 network during a node distress episode. By doing so, the signaling gateway routing node according to an embodiment of the present invention provides much needed network management service in the converged telephony – data network environment.

The functions for providing converged network management are described herein as modules or processes. It is understood that these modules or processes may be implemented as computer-executable instructions embodied in a computer-readable medium. Alternatively, the modules or

processes described herein may be implemented entirely in hardware. In yet another alternative embodiment, the modules or processes described herein may be implemented as a combination of hardware and software.

The processes and modules for providing converged network management functionality are described below as being associated with cards or subsystems within a gateway routing node. It is understood that these cards or subsystems include hardware for storing and executing the processes and modules. For example, each card or subsystems described below may include one or more microprocessors, such as an x86 microprocessor available from Intel Corporation, and associated memory.

Accordingly, it is an object of the present invention to provide a routing node that facilitates the inter-network communication of network management type messages in a converged network environment.

It is another object of the present invention to provide a system and method for use in a converged network environment whereby an Internet protocol (IP) device is able to divert traffic from one of a mated pair of signaling gateway (SG) nodes to the other in the event that one of the mated SG nodes is not able to access a particular destination point code.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby an IP device is able to audit the status of a point code associated with an SS7 signaling point.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby network

management information associated with a distressed SS7 node is distributed to concerned nodes in an IP network.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby an IP device may be notified of congestion in an SS7 sub-network component of the converged network environment.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby an IP device is able to assist in the abatement of congestion in an SS7 sub-network component of the converged network environment.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby an IP device is able to obtain SS7 User Part Unavailability status from in an SS7 sub-network component of the converged network environment.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby only one of a plurality of similar status request queries or polling messages sent by IP nodes is permitted to enter an SS7 network component of the converged network.

It is yet another object of the present invention to provide a system and method for use in a converged network environment whereby the receipt of a single SS7 network management message results in the distribution of multiple IP messages containing the SS7 network management message information.

Some of the objects of the invention having been stated hereinabove, other objects will become evident as the description proceeds, when taken in connection with the accompanying drawings as best described hereinbelow.

Brief Description of the Drawings

Figure 1 is a network diagram illustrating signaling message flow through a conventional converged telephony-data network.

Figure 2 is a schematic diagram of a conventional signaling system 7 (SS7) network management message structure.

Figure 3 is a network diagram illustrating conventional signaling message flow through a converged telephony-data network in the event of an SS7 signaling link failure.

Figure 4 is a block diagram of a conventional signaling gateway routing node architecture suitable for use with embodiments of the present invention.

Figure 5 is a schematic diagram of a signaling gateway routing node according to an embodiment of the present invention.

Figure 6 is a schematic diagram of an SS7 link interface module (LIM) illustrating message flow associated with the receipt of a network management message according to an embodiment of the present invention.

Figure 7 is diagram illustrating sample linkset and link selector tables associated with LIM **300** illustrated in Figure 6.

Figure 8 is a schematic diagram of an Internet protocol (IP) capable enhanced data communication module (eDCM) according to an embodiment of the present invention.

Figure 9 is a diagram illustrating a sample routing key table associated with eDCM **350** illustrated in Figure 8.

Figure 10 is a diagram illustrating a sample socket table associated with eDCM **350** illustrated in Figure 8.

Figure 11 is a network diagram that illustrates the flow of network management messages associated with an SS7 link failure episode according to an embodiment of the present invention.

Figure 12 is a schematic diagram of an eDCM including internal message flows associated with an SS7 link failure episode according to an embodiment of the present invention.

Figure 13 is a network diagram that illustrates message flows associated with a point code availability poll that is initiated by an IP node according to an embodiment of the present invention.

Figure 14 is a network diagram that illustrates message flows associated with a point code availability poll that is initiated by one of many IP nodes that are aliased to the same SS7 point code according to an embodiment of the present invention.

Figure 15 is a schematic diagram of an eDCM including internal message flows associated with a point code availability poll that is initiated by an IP node according to an embodiment of the present invention.

Figure 16 is a network diagram that illustrates message flows associated with simultaneous point code congestion polls that are initiated by multiple IP nodes according to an embodiment of the present invention.

Figure 17 is a network diagram that illustrates message flows associated with a point code congestion poll and subsequent distribution of a congestion response message according to an embodiment of the present invention.

Detailed Description of the Invention

Disclosed herein are several embodiments of the present invention, all of which include a network element that performs functions similar to that of a traditional telecommunications network packet routing switch, such as a signaling gateway routing node (SG). Each of the embodiments described and discussed below, employs an internal architecture similar to that of high performance signal transfer point (STP) and SG products which are marketed by the assignee of the present application as the Eagle® STP and IP^7 Secure Gateway™, respectively. A block diagram that generally illustrates the base internal architecture of the IP^7 Secure Gateway™ product is shown in Figure 4. A detailed description of the IP^7 Secure Gateway™ may be found in Tekelec publication PN/909-0767-01, Rev B, August 1999, entitled *Feature Notice IP^7 Secure Gateway™ Release 1.0*, the disclosure of which is incorporated by reference in its entirety. Similarly, a detailed description of the Eagle® STP may be found in the *Eagle® Feature Guide* PN/910-1225-01, Rev. B, January 1998, published by Tekelec, the disclosure of which is incorporated herein by

reference in its entirety. The specific functional components of an IP^7 Secure Gateway™ for transmitting and receiving transaction capabilities application part (TCAP) messages over an Internet Protocol (IP) network are described in commonly-assigned, co-pending International Patent Publication No. WO 00/35155, the disclosure of which is incorporated herein by reference in its entirety. Similarly, the functional components of an IP^7 Secure Gateway™ for transmitting and receiving ISDN user part (ISUP) messages over an Internet Protocol (IP) network are described in commonly-assigned, co-pending International Patent Publication No. WO 00/35156, the disclosure of which is also incorporated herein by reference in its entirety. As described in the above referenced *Feature Notice IP^7 Secure Gateway*™, an IP^7 Secure Gateway™ **250** includes the following subsystems: a Maintenance and Administration Subsystem (MAS) **252**; a communication subsystem **254** and an application subsystem **256**. MAS **252** provides maintenance communications, initial program load, peripheral services, alarm processing and system disks. Communication subsystem **254** includes an Interprocessor Message Transport (IMT) bus that is the main communication bus among all subsystems in the IP^7 Secure Gateway™ **250**. This high-speed communications system functions as two 125 Mbps counter-rotating serial buses.

Application subsystem **256** includes application cards that are capable of communicating with the other cards through the IMT buses. Numerous types of application cards can be incorporated into SG **250**, including but not limited to: a link interface module (LIM) **258** that interfaces with SS7 links and X.25 links,

an data communication module (DCM) **260** that provides an Internet Protocol (IP) interface using Transmission Control Protocol (TCP), and an application service module (ASM) **262** that provides global title translation, gateway screening, and other services. DCM **260** sends and receives Internet Protocol (IP) encapsulated SS7 messages over an IP network, as described in the above referenced *Feature Notice IP*^{7} *Secure Gateway*^{TM} *Release 1.0* publication.

Signaling Gateway Architecture

Figure 5 illustrates a signaling gateway (SG) routing node according to an embodiment of the present invention that is generally indicated by the numeral **270**. In Figure 5, SG routing node **270** is communicatively coupled to a signaling system 7 (SS7) signaling network **274** via an SS7 signaling link **276**, and to an Internet Protocol (IP) data network **278** via an IP connection **280**. It will be appreciated that these networks, taken together, constitute the functional network components of a converged telephony–data network. As such, telephony-related signaling information may be transported through either network sub-component. As further illustrated in Figure 5, SG routing node **270** includes a high-speed interprocessor message transport (IMT) communications bus **320**. Communicatively coupled to IMT bus **320** are a number of distributed processing modules or cards including: a pair of maintenance and administration subsystem processors (MASPs) **272**, an SS7 capable link interface module (LIM) **300**, and an Internet protocol (IP) capable enhanced

data communication module (eDCM) **350**. These modules are physically connected to the IMT bus **320** such that signaling and other types of messages may be routed internally between all active cards or modules. For simplicity of illustration, only a single LIM **300** and DCM **350** are included in Figure 5. However, it should be appreciated that the distributed, multi-processor architecture of the SG routing node **270** facilitates the deployment of multiple LIM, DCM and other cards, all of which could be simultaneously connected to and communicating via IMT bus **320**.

From a hardware perspective, LIM **300** and eDCM **350** may each comprise a printed circuit board physically connected to IMT bus **320**. Each printed circuit board may include a communication processor programmed to send and receive messages via IMT bus **320**. Each printed circuit board may also include an application processor programmed to perform various functions. For example, the application processor of eDCM **350** may be programmed to perform the functions described herein for sending SS7 network management messages to IP nodes.

MASP pair **272** implement the maintenance and administration subsystem functions described above. As MASP pair **272** are not particularly relevant to a discussion of the flexible routing attributes of the present invention, a detailed discussion of their function is not provided herein. For a comprehensive discussion of additional MASP operations and functionality, the above-referenced Tekelec IP^7 Secure Gateway™ and Eagle® STP publications can be consulted.

Given the SG routing node internal architecture shown in Figure 5 and briefly discussed above, it will be appreciated that the most fundamental operation of the SG **270** involves the receipt of a signaling message at LIM **300** from an SS7 network and the subsequent internal routing of this message to eDCM **350** for transmission into the IP network **278**, and vice versa.

Link Interface Module (LIM) Architecture

Referring to Figure 6 and focusing now on LIM card functionality, it will be appreciated that LIM **300** is comprised of a number of sub-component processes including, but not limited to: an SS7 message transfer part (MTP) level 1 process **302**, an SS7 message transfer part (MTP) level 2 process **304**, an I/O buffer or queue **306**, an SS7 MTP level 3 message handling and discrimination (HMDC) process **308**, a message handling and routing (HMRT) process **310**, and a message handling and distribution (HMDT) process **312**. MTP level 1 process **302** is adapted to provide the facilities necessary to send and receive digital data over a particular physical media / physical interface, such as a DS0 type communication link. Working in conjunction with the MTP level 1 process **302**, MTP level 2 process **304** provides for basic error detection/correction and sequenced delivery of all SS7 message packets. I/O queue **306** provides for temporary buffering of incoming and outgoing SS7 signaling message packets. HMDC process **308** receives signaling messages from the lower processing layers and performs a discrimination function, effectively determining whether an incoming SS7 message packet requires

internal processing or is simply to be through switched. HMRT process **310** is adapted to receive and route messages from the discrimination process **308** that do not require further processing at the SG and are simply to be through switched. HMDT process **312** is adapted to facilitate the internal routing of SS7 message packets, received from the discrimination process **308**, that do require additional SG based processing prior to final routing.

Also included on LIM **300** are a functional group of processes that are generally associated with the routing of signaling messages, at both an internal and external level. That is, the information contained in this group of functional processes comprises a set of rules for the routing of a received signaling message within an associated signaling network. Tightly coupled or closely related to this set of network routing rules is an associated set of rules that describe and define the routing of the signaling message within the SG node.

As indicated in Figure 6, these functional routing processes include a link selection manager (LSM) process **314**, a linkset selector table **316**, and a link selector table **318**. Tables **316** and **318** contain signaling route and signaling route status information, along with internal IMT bus routing information. As mentioned above, these tables facilitate the overall routing of an SS7 signaling message received by the LIM **300**. LSM process **314** is adapted to perform a number of functions including the administration of routing data within the linkset and link selector tables **316** and **318**, respectively. LSM **314** is further adapted to notify other communication modules, generally within the SG, and coupled to IMT bus **320** of changes in the status of links and other nodes in the

SS7 network. In one embodiment of the present invention, LSM **314** is adapted to receive an SS7 network management (NM) message, use information contained within the NM message to update route status information in linkset selector table **316** and link selector table **318**, respectively, and subsequently distribute the NM information to other communication modules connected to IMT bus **320**.

Figure 7 includes sample table structures and data associated with linkset and link selector tables **316** and **318**, respectively. Example linkset selector table **316** includes a key field that is used to effectively index the data table. This index is comprised of an SS7 destination point code (DPC) **322**. Linkset selector table **316** also includes a route cost field **324**, a linkset status field **326**, an adjacent node status field **328**, an overall status field **330**, and a linkset identifier or pointer field **332**.

Link selector table **318** includes a compound key that is comprised of a linkset identifier **336** and a signaling link field **338**. Link selector table **318** also includes an IMT address field **340**, which contains IMT bus address information associated with communication modules that are connected to the IMT bus **320**. More particularly, a record in the table **318** includes an IMT address value that is associated with the communication module that supports the specific link identified in the record key. For example, as shown in Figure 7, link 0 of linkset 1 resides on a communication module that has an IMT bus address of 1305. Furthermore a link status field **342**, indicates that link 0 of linkset 1 is available for service.

It will be appreciated, as generally indicated in Figure 6, that a first database lookup in linkset selector table **316** returns an index value or pointer that is subsequently used in a second database lookup in link selector table **318**. The ultimate result of this two-stage lookup procedure is an IMT bus address associated with a communication module. It will also be appreciated that any number of database configurations or structures could be effectively employed to achieve a functionality similar to that described above. The database table structures shown in Figure 7 merely illustrate one example implementation.

Once again, it should be appreciated that a LIM card may contain more functional processes than those described above. The above discussion is limited to LIM functionality associated with the basic processing of inbound SS7 signaling messages.

Enhanced Data Communication Module (eDCM) Architecture

Figure 8 illustrates an enhanced data communication module (eDCM) according to an embodiment of the present invention, generally indicated by the numeral **350**. eDCM **350** is connected to IMT communication bus **320** and is comprised of a number of functional modules or processes. These modules include: a layers 1 and 2 module **352**, a layers 3 and 4 module **354**, an I/O buffer or queue **358**, an HMDC (message discrimination) process **360**, an HMDT (message distribution) process **362**, an HMRT (message routing)

process **364**, a link selection manager process **366**, a linkset selector table **368**, and a link selector table **370**.

Layers 1 and 2 module **352** provides physical and data link layer functions for upper layer services. For example, layers 1 and 2 module **352** may implement a digital communication link that delivers bits over a physical medium. In addition, layers 1 and 2 module **352** may frame packets so that the receiver can recover the packets and can arrange for retransmission of packets.

Layers 3 and 4 module **354** provides network and transport layer services for incoming and outgoing packets. Exemplary network layer services that may be provided by layers 3 and 4 module **354** include routing packets from source to destination along a path that may comprise a number of links. Exemplary transport layer services that may be provided include message sequencing, timeouts, and retransmissions.

In addition to the conventional layers 3 and 4 functions, module **354** may translate between SS7 and IP address schemes. In order to perform such translation, layer 3 process **354** may utilize the procedures described in one or more of the existing standards for such conversions, such as that described in IETF Internet Draft draft-benedyk-sigtran-tali-01.txt, the disclosure of which is incorporated herein by reference in its entirety. Alternatively, such a mapping may be performed using the packet formats as described in RFC 2960: Stream Control Transmission Protocol, October 2000, the disclosure of which is incorporated herein by reference in its entirety.

I/O queue **358** provides for temporary buffering of incoming and outgoing IP signaling message packets. HMDC process **360** receives signaling message packets from the lower processing layers and performs a discrimination function, effectively determining whether an incoming IP message packet requires internal processing or is simply to be through switched. HMRT process **364** is adapted to receive and route messages from message discrimination process **360** that do not require further processing at the SG and are simply to be through switched. HMDT process **362** is adapted to facilitate the internal routing of IP message packets, received from message discrimination process **360**, that do require additional SG based processing prior to final routing.

Link selection manager process **366** is adapted to perform a number of functions including the administration of routing data within the linkset and link selector tables **368** and **370**, respectively. It will be appreciated that the linkset and link selector tables **368** and **370** are similar in structure and form to the corresponding LIM based databases illustrated in Figure 7. As such, these linkset and link selector tables contain signaling route and signaling route status information, along with internal IMT bus routing instructions. LSM **360** is further adapted to notify other communication modules, generally within the SG, and coupled to IMT bus **320** of changes in the status of links and other nodes in both the SS7 and IP network components. In one embodiment of the present invention, LSM **360** is adapted to receive an IP-based TALI or SCTP network management (NM) message, use information contained within the NM message

to update route status information in the linkset and link selector tables **368** and **370**, respectively, and subsequently distribute the NM information to other communication modules connected to IMT bus **320**.

It will be appreciated from Figure 8 that layers 3 and 4 process **354** is further comprised of an inbound message manager process **372**, an MTP primitive controller process **374**, an outbound message manager process **376**, a routing key database **378**, and a socket database **380**. An incoming IP message from IP network **278** is received by inbound message manager process **372** which subsequently examines the message packet and determines the appropriate response or processing action that is required. For instance, if the incoming IP signaling message packet is a call setup type message, the inbound message manager (IMM) process **372** may simply de-capsulate the SS7 portion of the message packet and subsequently pass the message to the I/O queue **358**. If, however, the incoming IP signaling message packet is a network management information request or polling type message, IMM process **372** may extract relevant information from the message packet and consult MTP primitive controller process **374**. MTP primitive controller process **374** examines the extracted information and generates an appropriate, related SS7 MTP message that can be routed to and interpreted by other SS7 nodes in an SS7 network. In some instances, the MTP primitive controller process **374** need not be consulted, and in such cases the IMM process **372** will respond directly. The particular response provided depends on the

character of the original received IP network management message, and several such response scenarios will be discussed in more detail below.

Outbound message manager (OMM) process **376** is adapted to receive an outbound data packet from I/O queue **358** and begin the process of preparing the data packet for transmission into an IP network. As discussed above, exemplary packet structures that may be used to transmit SS7 messages over an IP network include TALI over TCP/IP or SCTP/IP. OMM process **360** receives a data packet from I/O queue **358** and, using information contained in the data packet, consults the routing key and socket tables **378** and **380**, respectively, for appropriate routing address information.

Figure 9 illustrates an example of routing key table **378**. More particularly, sample routing key table **378** is comprised of multiple routing key fields including: an SS7 destination point code (DPC) **382**, an SS7 origination point code (OPC) **384**, a service indicator (SI) **386**, a circuit identification code (CIC) **388**, and a sub-system number (SSN) **390**. Those skilled in the art of SS7 network operation will appreciate that such routing keys are commonly employed in SS7 routing nodes (i.e., STPs) to determine how and to where a signaling message packet should be routed. It will also be appreciated that many different combinations of signaling message parameters may be used to form a routing key, and as such, the particular structure presented in Figure 9 is simply one of many possible routing key table structures.

Associated with each routing key record in the routing key table **378** is a socket identifier or pointer **392**. This socket identifier is used to access data in

the associated socket table **380**, shown in Figure 10. Referring to Figure 10, socket table **380** includes information that defines a particular IP socket connection. More particularly, table **380** includes a socket identifier **394**, and associated local IP addresses and port numbers **395** and distant IP addresses and port numbers **396**. Socket table **380** also includes a socket status field **397**, which contains availability status information related to each socket that is defined in the table.

Once again, it will be appreciated that the database structures and tables described above are merely illustrative of the types of data that can be employed to provide the functionality of an eDCM of the present invention.

SG Functionality Associated With an SS7 Node or Link Failure

Shown in Figure 11 is a simplified converged SS7 – IP communication network, generally indicated by the numeral **400**. Network **400** is comprised of a number of SS7 network elements including a service control point (SCP) **104** and a signal transfer point (STP) **106**. Converged network **400** also includes an IP network **110** and a number of IP connected network elements such as a database server node (DBS) **112**, a first media gateway controller (MGC) **114**, and a second MGC node **116**.

As further indicated in Figure 11, it will be appreciated that each of the SS7 network elements is assigned a unique SS7 address or point code (PC), such that SCP **104** is identified in the SS7 network as PC = 6-1-1, STP **106** is identified as PC = 5-1-1. In a similar manner, each IP network element is

assigned a unique IP address, such that DBS node **112** is identified in the IP network as IP = 10.10.10.1: Port 24, MGC **114** is identified as IP = 10.10.10.2: Port 12, and MGC **116** is identified as IP = 10.10.10.3: Port 54. In the converged network environment, it will be further appreciated that each IP network element is assigned an SS7 network address or alias, such that DBS node **112** is also identified by the SS7 point code PC = 3-1-1, MGC **114** is identified by PC = 3-1-2, and MGC **116** is identified by PC = 3-1-3.

Also included in converged network **400** is a signaling gateway (SG) routing node **402** of the present invention. As such, it will be appreciated that SG **402** includes both LIM and eDCM communication modules, as described above. In the simplified network diagram shown in Figure 11, SG **402** communicates with adjacent SS7 STP node **106** via a single SS7 signaling link. SG **402** communicates with IP DBS node **112**, IP MGC node **114**, and IP MGC node **116** via a plurality of IP sockets. Furthermore, in the examples discussed herein, it is assumed that SG **402** and the IP nodes connected thereto all implement an appropriate stream-oriented communication protocol, such as TALI over TCP/IP or SCTP/IP. Again, it will be appreciated that a number of functionally similar protocols that provide reliable, stream-oriented communication could also be employed by the SG and IP nodes to facilitate communication.

The particular scenario presented in Figure 11 corresponds to the case where a node in an SS7 network fails or becomes inaccessible. Such a situation may arise from one or more signaling link failures or possibly a higher

level failure within the node. In any event, in the example shown in Figure 11, SCP node **104** is assumed to experience a signaling link failure that effectively isolates the node from all other elements in the converged network. Upon determination that SCP node **104** is unavailable, SG **402** generates an SS7 transfer prohibited (TFP) network management message and subsequently sends copies of the TFP message to other SS7 nodes in the network. In this particular example, STP **106** is notified of the problem with SCP node **104** via the TFP message. Once notified and made aware of the unavailable status of SCP **104**, SS7 nodes will not attempt to route SS7 signaling messages to SCP **104** until such time as they are again notified by SG **402** that SCP **104** has recovered.

Prior to SG **402** according to an embodiment of the present invention, an efficient and effective technique whereby IP nodes in the converged network could take advantage of network management information generated within the SS7 component of a converged network environment did not exist. It is at this point that one of the significant advantages of the present invention will be appreciated. More particularly, it will be appreciated from the message flows illustrated in Figure 11 that SG **402** is adapted to generate a related, IP-formatted, TALI- or SCTP-based point code unavailable (PCUA) message that is effectively and efficiently distributed to relevant nodes in the IP component of the converged network environment. As such, SG **402** of the present invention is capable of generating and distributing a plurality of IP network management

messages that are associated with or analogous to an SS7 network management message (e.g., a TFP message).

Upon receipt of a TALI PCUA message, DBS node **112**, MGC node **114**, and MGC node **116** are effectively notified of the SS7 network difficulty and further transmission of IP originated signaling messages that would be destined for SCP **104** is halted.

eDCM Response To An SS7 TFP Network Management Message

Figure 12 illustrates eDCM communication module **350** and relevant message flows associated with the SS7 node or link failure discussed above and generally illustrated in Figure 11. For the purposes of example, it is assumed that the SS7 TFP network management message is generated at SG **402** by the SS7 link interface module **300**(illustrated in Figure 6). TFP message creation and subsequent distribution is performed by one or more MTP level 3 processes. In any event, a TFP message is generated and route availability information is updated in linkset and link selector tables **316** and **318**, respectively. More particularly, route status information associated with failed SCP node **104** needs to be updated to reflect the SCP node's unavailable state. As such, LSM **314** facilitates the updating of linkset and link selector tables **316** and **318**, respectively.

HMDT process **312** determines that other communication modules connected to IMT bus **320** also need to update their local linkset and link selector tables, and consequently distributes copies of the TFP network

management message to other communication modules in the SG via IMT bus **320**.

Returning to Figure 12, it will be appreciated that a copy of the TFP network management message or at least a portion of the information originally contained therein is received at eDCM **350** via IMT bus **320**. More particularly, the TFP message is received by the local eDCM link selection manager (LSM) process **366**, which in turn uses the network management information to update route and link status information contained in linkset and link selector databases **368** and **370**, respectively. LSM **390** forwards the TFP message to MTP primitive controller **374** and OMM **376** processes which determine, based on information contained in the routing key and socket tables **378** and **380**, respectively, that there are several provisioned IP communication links which have the capability of receiving IP node originated signaling messages that might be destined for the failed SCP node **104**. In the example shown in Figure 11, the affected IP nodes include DBS node **112**, MGC node **114**, and MGC node **116**. Consequently, these IP nodes need to be notified of the unavailable status of SCP node **104**.

It will be appreciated that information may be stored in the routing key and socket databases that indicate whether a particular IP node prefers to receive broadcast type network management messages or instead to receive network management messages associated with a more selective response method. In the event that a network management (NM) message requiring broadcast distribution is received by SG **402**, all concerned nodes or point

codes that are configured to accept broadcast type messages will receive the NM message, such as generally indicated in Figure 11.

In the event that a NM message is received by SG **402** that does not require broadcast distribution, a more selective response method may be employed. For example, a NM message could be received by SG **402** which does not require broadcast distribution and which is specifically addressed to PC = 3-1-1, the point code of DBS node **112**. In such a case, the NM message may be selectively distributed to DBS node **112**, as shown in Figure 13. As multiple sockets may be aliased to a single SS7 point code, it will be appreciated that in certain instances, a selective response method of the present invention may result in the distribution of a NM message to multiple IP nodes which all share the same SS7 point code address. In any event, the present invention is adapted to accommodate both broadcast and selective response type methods.

As such, LSM **366** passes the TFP network management message to the outbound message manager (OMM) process **376**, via I/O queue **358**. Using information contained in the TFP message, OMM **376** consults MTP primitive controller process **374** in order to formulate a IP-based network management message that is equivalent or related to the original SS7 TFP network management message. Once again, in this embodiment, the IP-based network management protocol may be TALI or SCTP. However, any stream-oriented mechanism for reliably transporting SS7 messages over an IP network may be employed.

MTP primitive controller process **372** returns an IP-based TALI or SCTP point code unavailable (PCUA) network management message to OMM **376**. In response, OMM **376** consults the routing key and socket tables **378** and **380**, respectively, to determine the particular socket or sockets over which the PCUA message should be transmitted. In the example routing key table **378** shown in Figure 9, there are three IP sockets that support communication with SCP node **104**. These sockets are identified as sock1, sock2, and sock3. Consequently, OMM process **376** replicates the PCUA message so as to effectively produce one copy of the PCUA message for each of the three sockets. Each copy of the PCUA message is appropriately addressed, using IP address and TCP port information returned by the socket table **380**. The three PCUA messages are subsequently passed through layers 1 and 2 processing and transmitted into the IP network **110** where they are eventually received by the three IP nodes: DBS **112**, MGC **114**, and MGC **116**. Again, it will be appreciated that upon receipt of a PCUA message, each of the above mentioned IP nodes is made aware of the SCP **104** node or link failure, and further transmission of signaling messages from these IP nodes to SCP **104** is halted. As such SS7 network management information has effectively been communicated to and acted upon by nodes in an IP network.

SG Functionality Associated With IP Availability Polling

Continuing with the failed SS7 node scenario presented in Figure 11 and discussed in detail above, Figure 13 illustrates a subsequent attempt by IP-

based DBS node **112** to obtain information regarding the availability status of the failed SS7 SCP node **104**.

More particularly, it will be appreciated from the message flows illustrated in Figure 13 that DBS node **112** is adapted to periodically poll the SS7 network component of the converged network **400** regarding the availability status of SCP **104**. In the embodiment illustrated, such availability status polling may be accomplished or facilitated via a point code availability audit (PCAUD) TALI- or SCTP-formatted message.

As indicated in Figure 13, DBS node **112** generates and transmits a PCAUD message into IP network **110**. The PCAUD message is received and subsequently processed by SG **402**. In the particular example shown in Figure 13, it is assumed that SCP **104** continues to be unavailable for service and SG **402** consequently responds with a TALI or SCTP point code unavailable (PCUA) message. It will be appreciated that STP **106**, which is the routing node immediately adjacent the failed SCP **104**, is not consulted for SCP **104** status. SG **402** of the present invention is adapted to utilize on-board route status information when generating a response to a PCAUD or similar type availability status poll from an IP-based node. As indicated in Figure 13, it will also be appreciated that SG **402** responds with a single PCUA message that is sent to the PCAUD message originator over the socket through which the PCAUD message was received.

It will be appreciated that multiple IP nodes and / or socket connections may be aliased to the same SS7 point code in a converged network

environment, as described in commonly-assigned, co-pending International Patent Publication No. WO 00/60812, the disclosure of which is incorporated herein by reference in its entirety. Such a scenario is generally illustrated in Figure 14, and it will be appreciated that in such an aliasing configuration SG **402** is adapted to respond only to the specific DBS node that originated the PCAUD polling message. By doing so, network management signaling traffic within IP network **110** is kept to a minimum, thereby avoiding congestive conditions within the IP network. If a converged network operator were so inclined, however, SG **402** could be configured to respond to all of the IP nodes (i.e., DBS nodes **112a**, **112b**, and **112c**) that are aliased to the SS7 point code 3-1-1.

eDCM Functionality Related To IP Availability Polling

Figure 15 illustrates eDCM communication module **350**, and relevant message flows associated with the SS7 node availability poll discussed above and generally illustrated in Figures 13 and 14. For the purposes of example, it is assumed that the SS7 PCAUD network management message is received at SG **402** by eDCM communication module **350**. As in previous figures, the dashed lines represent routing of the inbound messages, while the solid lines represent communication between processes. As generally indicated in Figure 15, the PCAUD message is received via IP layers 1 and 2 process **352**, and is subsequently processed and directed to IP layers 3 and 4 process **354**.

Within layers 3 and 4 process **354**, the PCAUD message is received by inbound message manager (IMM) process **372**. In one embodiment, IMM process **372** consults linkset selection manager (LSM) process **366**, which examines information contained in the received PCAUD network management message and determines the availability status of the SS7 node in question. This SS7 point code availability status determination is facilitated by SS7 point code / route status information that is maintained in link selector table **370**.

For the purposes of this example, it is assumed that the point code / route status information returned by LSM process **366** indicates that SCP node **104** is still unavailable. This status information is returned to IMM process **372** which subsequently generates a TALI PCUA network management response message and passes this message to outbound message manager (OMM) process **376** via I/O queue **358**. It will be appreciated that in this case, information identifying the originating socket over which the PCAUD message was received is placed in the PCUA message packet by IMM process **372**. Consequently, OMM process **376** need not necessarily consult the routing key and socket databases **378** and **380**, respectively, to determine the particular IP socket or sockets over which the PCUA message should be transmitted. Instead the PCUA message packet is passed to layers 1 and 2 **352** and subsequently transmitted to and received by DBS node **112**, as shown in Figure 13.

Again, it will be appreciated that upon receipt of a PCUA message, DBS node **112** is again made aware of the continuing SCP **104** node or link failure,

and transmission of signaling messages from this IP node to SCP **104** remains suspended.

SG Functionality Related To IP Congestion Poll Filtering

Shown in Figure 16 is a converged network scenario that involves an SS7 node that is in a congested state. More particularly, converged network **420** includes SCP node **104** that is experiencing congestion, possibly due to an abnormally high volume of signaling traffic across the SS7 communication link that connects the node to STP **106**. It will be appreciated that upon receipt of an MSU destined for the congested SCP **104**, STP **106** would typically generate an SS7 transfer controlled (TFC) network management message and subsequently notifies the MSU originator of the congested status of SCP **104**. It should also be appreciated that this initial SS7 TFC network management message is not broadcast to all concerned IP nodes in a manner analogous to that described above for TFP type messages. With TFC type congestion NM messages, more selective response methods may be employed by SG **402**.

Subsequent to the initial TFC notification, an affected IP node is adapted to periodically poll the congested SS7 node in an attempt to determine when the congestion has abated, and normal routing can resume. The particular example scenario illustrated in Figure 16 involves the simultaneous or near simultaneous polling by the three IP nodes: DBS **112**; MGC **114**; and MGC **116**. Once again, assuming that a TALI or SCTP signaling protocol is employed, the IP node generated polling messages are in the form of a congestion status

audit (CONGAUD) type network management message. As indicated in Figure 16, while all three independently generated CONGAUD messages are received at SG **402** simultaneously or nearly simultaneously, only one SS7 route set congestion test (RCT) message is generated by SG **402** and subsequently routed to STP **106**. As such, SG **402** effectively filters redundant congestion status polls received from the IP network **110**, and consequently reduces congestion on the SS7 signaling link that connects SG **402** and STP **106**.

With regard to eDCM operation in such a scenario, it will be appreciated that in one embodiment such filtering is accomplished by an inbound message manger (IMM) process which is similar to the IMM processes previously disclosed herein. More particularly, an eDCM based IMM process is adapted to utilize a timer such that only a single CONGAUD message related to a specific SS7 node is conveyed through to the SS7 network in a pre-determined time period. A CONGAUD message that satisfies the time-filter criteria would be processed by an MTP primitive controller similar to those discussed previously, which would produce an equivalent, related SS7 RCT network management message. In a manner similar to those already described in detail herein, the SS7 RCT message would be internally routed within the SG to an appropriate LIM module via an IMT bus, where the RCT message would be transmitted to STP **106**.

SG Functionality Related To Congestion Response Message Distribution

Shown in Figure 17 is a converged network scenario that is related to that presented in Figure 16 and discussed in detail above. Once again, converged network **430** includes SCP node **104** that is experiencing congestion, possibly due to an abnormally high volume of signaling traffic across the SS7 communication link that connects the node to STP **106**. As discussed previously, STP **106** would have previously generated an initial SS7 transfer controlled (TFC) network management message and subsequently notified the DBS nodes corresponding to SS7 PC = 1-1-1 (i.e., nodes **112a** and **112b**) of the congested status of SCP **104**.

Subsequent to the initial TFC notification, the two affected IP nodes are adapted to periodically poll the congested SS7 node in an attempt to determine if the congestion at SCP **104** has abated, and normal routing can resume. The particular example scenario illustrated in Figure 17 involves a congestion status audit (CONGAUD) network management message that is originated by IP based DBS node **112a**. As indicated in Figure 17, the CONGAUD message is received at SG **402** and an SS7 route set congestion test (RCT) message is subsequently generated at SG **402** in a manner similar to that previously described. The RCT message is routed to STP **106**, which determines that SCP **104** is still congested and subsequently responds to SG **402** with a TFC network management message that effectively confirms the congested status of SCP node **104**.

In much the same manner as the TFP message in the example scenario presented in Figure 11 and described in detail above, the TFC message is received by a LIM in the SG **402** and subsequently routed internally via an IMT bus to an eDCM communication module. Again, at the eDCM module, the SS7 TFC network management message flow is similar to that generally illustrated in Figure 12.

As such, it will be appreciated that a copy of the TFC network management message or at least a portion of the information originally contained therein is received at eDCM **350** via IMT bus **320**. MTP primitive controller **358** and OMM **360** determine, based on the information contained in the routing key and socket databases **362** and **364**, respectively, that there are two provisioned IP communication sockets which are aliased to the point code (i.e., PC = 1-1-1) that generated the original congestion audit NM message. In the example shown in Figure 17, the concerned IP nodes include DBS nodes **112a** and **112b**.

Returning to the discussion of eDCM operation, as indicated in Figure 12, LSM **390** passes the TFC network management message to the outbound message manager (OMM) process **360**, via I/O queue **376**. Using information contained in the TFC message, OMM **360** consults MTP primitive controller process **358** in order to formulate a IP-based network management message that is equivalent or related to the original SS7 TFC network management message. Once again, in this embodiment, it is assumed that the IP-based network management protocol is TALI- or SCTP-based. However, other

reliable stream-oriented procedures may be used. In addition, any application layer protocol, such as SIP, may be used to communicate with the IP nodes.

MTP primitive controller process **358** returns an IP-based TALI point code congested (CONGLVL) network management message to OMM **360**. It will be appreciated that a CONGLVL type congestion message may include information that indicates the degree or level of congestion. In any event, OMM **360** subsequently consults the routing key and socket databases **362** and **364**, respectively, to determine the particular socket or sockets over which the CONGLVL message should be transmitted. In the example routing key table **362** shown in Figure 9, there are two sockets that support communication with SCP node **104**. These sockets are identified as sock4, and sock5. Consequently, OMM process **360** replicates the CONGLVL message so as to effectively produce one copy of the CONGLVL message for each of the two sockets. Each copy of the CONGLVL message is appropriately addressed, using IP address and TCP port information returned by the socket database process **364**. The two CONGLVL messages are subsequently passed through IP level 1 processing and transmitted into the IP network **110** where they are eventually received by the two IP nodes: DBS **112a** and **112b**. Again, it will be appreciated that upon receipt of a CONGLVL message, each of the above mentioned IP nodes is made aware of the congested status of SCP **104** node so that alternate routes may be employed, if possible. It will be appreciated that MGC node **114** and MGC node **116** do not receive copies of the congestion response message, as they are not associated with the PC 1-1-1.

Again, it should be noted that other signaling protocols and network management messages may be employed within the context of the present invention. Those skilled in the art of SS7 telecommunication networks will appreciate that functionality similar to that described above could be implement at a cluster routing level. Such a cluster routing scenario would involve different SS7 MTP network management messages and their corresponding TALI or SCTP equivalents, however the basic processing within a SG of the present invention would be similar. Again, it is the ability to effectively and efficiently communicate network management type information between different network components in a converged network environment that is key to the present invention. It will also be appreciated that various details of the invention may be changed without departing from the scope of the invention. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation—the invention being defined by the claims.